LISTING OF THE CLAIMS

CLAIMS

1. (Currently amended) A method for attestation comprising generating a user attestation-signature value for use with a verification computer, the user attestation-signature value corresponding to at least one attribute (A, B, C, D), each with an attribute value (w, x, y, z), none, one, or more of the attribute values (w, y) remaining anonymous for transactions performable by a user device having a security module with the verification computer, the step of generating comprising the steps of:

- providing a user public key and a proof value that demonstrates that the user public key was validly derived from a module public key of the security module;

- receiving from an attester computer :

(I) an attestation value having the at least one attribute (A, B, C, D) with its attribute value (w, x, y, z), none, one or more of the attribute values (x, y) remaining unknown to the attester computer,

the attestation value being derived from an attester secret key , a user public key, and none, one, or more attester determined attribute values (w, z),

the user public key inherently comprising none, one, or more user determined attribute values (x, y), and

(II) at least one of the attester determined attribute values (w, z); and

- deriving the user attestation-signature value from the attestation value and a security module attestation value provided by the security module,

wherein:

it is verifiable whether or not (i) the user attestation-signature value was validly derived from the security module attestation value and the attestation value, and that (ii) the attestation value is associated with a subset (B, D) of at least one attribute, each attribute in the subset (B, D) having a revealed attribute value (x, z);

the step of deriving the user attestation-signature value further comprises the steps of:

receiving from the security module a first security module attestation value,

deriving an intermediate user attestation-signature value from the first security module attestation value under use of an attester public key and a hash function;

providing the intermediate user attestation-signature value to the security module,

receiving from the security module a part of the user attestation-signature value, and

calculating by the user device further parts of the user attestation-signature value using none, one, or more of the attribute values (w, y), the received part of the user attestation-signature value, the user public key, and the attester public key;

the user public key is derived from the module public key by using the attester public key and the one or more of the attribute values (x, y);

the user device provides encryptions under a trusted third party's public key of one or more of the attribute values (w, y) that remain unknown to the verification computer;

the user public key is derived from the module public key by using the attester public key and the one or more of the attribute values (x, y);

the user deviceprovides encryptions under a trusted third party's public key of one or more of the attribute values (w, y) that remain unknown to the verification computer;

the user device provides encryptions under a trusted third party's public key of one or more of the attribute values (w, y) that remain unknown to the verification computer;

the step of deriving the user attestation-signature valuefurther comprises the steps of:

receiving from the security module a first security module attestation value,

deriving an intermediate user attestation-signature value from the first security module attestation value under use of an attester public key and a hash function,

providing the intermediate user attestation-signature value to the security module;

receiving from the security module a part of the user attestation-signature value, and

calculating by the user device further parts of the user attestation-signature value using none, one, or more of the attribute values (w, y), the received part of the user attestation-signature value, the user public key, and the attester public key; and

the user public key is derived from the module public key by using the attester public key and the one or more of the attribute values (x, y); and

the user device provides encryptions under a trusted third party's public key of one or more of the attribute values (w, y) that remain unknown to the verification computer.

2. - 20. (Canceled)